

REMARKS

By this Amendment, claims 6, 8, 11, 12, 16, 23, 25 and 28 are amended. Claims 1-5, 7, 9-10, 13-15, 17-22, 24 and 26-27 remain in the application. Thus, claims 1-28 are active in the application. Reexamination and reconsideration of the application are respectfully requested.

Minor editorial revisions were made to claims 6, 8, 11, 12, 16, 23, 25 and 28 in order to make obviously necessary clerical corrections in view of the amendments to the claims made in the December 17, 2004 Amendment. Furthermore, claims 25 and 28 have been amended to correct clerical errors denoting to which base claim these claim depend. Claim 25 further defines the data terminal equipment according to claim 1, but claim 25, as presented in the December 17, 2004 Amendment, incorrectly recited claim 16, instead of claim 1, as its base claim. Similarly, claim 28 further defines the program according to claim 16, but claim 28, as presented in the December 17, 2004 Amendment, incorrectly recited claim 6, instead of claim 16, as its base claim.

The Applicants respectfully submit that the minor editorial revisions made to claims 6, 8, 11, 12, 16, 23, 25 and 28 are of such a minor nature that they do not raise new issues that would require further consideration and/or search, or raise the issue of new matter. Accordingly, the Applicants respectfully request entry of the amendments to claims 6, 8, 11, 12, 16, 23, 25 and 28 in response to the final Office Action.

In item 3 on page 2 of the Office Action, claims 1-4, 6-9, 11-14 and 16-19 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Palage et al. (U.S. 6,247,133) in view of Katz et al. (U.S. 5,926,624). This rejection is respectfully traversed for the following reasons.

In conventional systems and methods, as described in the Description of the Background Art section of the specification, an information user of the data terminal equipment cannot authorize the authenticity of content data received from a server until after the information user has actually received the content data from the server. Accordingly, in the conventional systems and methods, once a user has received unauthentic content data, the information user either has wasted his or her time acquiring the unauthorized content data, or the information user may become a victim of so-

called cracking, where, for example, the information user's personal information may be stolen.

Furthermore, in the conventional systems and methods, the information user must access a third-party authorization agency, which authorizes whether the content data stored on the server is authentic, in order to determine whether or not any received content data is authentic.

Accordingly, an object of the present invention is to provide a user data terminal equipment which is capable of authenticating content data before actually retrieving the content data from a server. Another object of the present invention is to provide a user data terminal equipment which is capable of authenticating content data without accessing a third-party authorization agency.

The present invention achieves the stated objects by providing a data terminal equipment and method for use in an information providing system where a server provides content data stored therein to the data terminal, which is placed on an information user's side for retrieving the content data through a communications network.

As described, for example, in lines 11-12 on page 12 of the specification, index data indicating the content data is received by the data terminal equipment prior to the data terminal equipment receiving the content data. Next, an authentication part of the data terminal equipment authenticates the yet-to-be received content data by using the retrieved index data related to the content data. Then, as described, for example, in lines 13-22 on page 16 of the specification, a content retrieval part of the data terminal equipment transmits a retrieval request for the authenticated content data to the server only if the authentication part has confirmed authenticity of the content data, and then receives the authenticated content data from the server.

Accordingly, by receiving the content data from the server only after the content data has been authorized by using retrieved index data related to the content data, the present invention prevents the an information user of the data terminal equipment from receiving unauthorized content data. Therefore, the information user is prevented from browsing unauthorized content data.

Claim 1 recites the data terminal equipment as comprising a content retrieval part operable to transmit a retrieval request only if the authentication part has confirmed authenticity of the content data, and to receive the authenticated content data from the server..

Claims 6, 11 and 16 each recite transmitting a retrieval request for retrieving the content data to the server only if authenticity of the content data has been confirmed, and receiving the authenticated content data from the server.

In lines 3-5 on page 3 of the Office Action, the Examiner acknowledged that Palage et al. fails to disclose or suggest that content data retrieval is only requested if the authentication part has confirmed the authenticity of the content data.

The Examiner applied Katz et al. o cure the deficiencies of Palage et al. In particular, with reference to Column 8, lines 32-40 and Column 11, 47-54, the Examiner contended that Katz et al. discloses that content data retrieval is only requested if the authentication part has confirmed the authenticity of the content data.

The Applicants respectfully submit that the Examiner's contention is incorrect for the following reasons.

Katz et al. discloses a digital information library where a library server 260 securely provides digital information library data to a client computer system 214 and a portable playback device (player) 212, 226 removably connected to the client computer system 214 (see Column 2, line 66 to Column 3, line 5 and Figures 2 and 4-6).

Katz et al. discloses that a point-to-point authentication protocol is performed in which the library server 260 must verify that the requesting client system 214 is an authorized client, and the client computer system must verify that the library server 260 is an authorized provider of the library data. Furthermore, another point-to-point authentication protocol is performed between the library server 260 and the players 212, 226, where the library server utilizes a set of identifiers (player IDs) for the players 212, 226 to verify that the players 212, 226 are authorized to receive selected download data from the library server 260. In particular, a library server digital signature is appended to the downloaded data for use by the players 212, 226 to verify that the downloaded data was originated by an authorized library server (see Column 11, lines 34-51).

Katz et al. describes the specific verification process of the downloaded data as follows:

1. For selected data blocks generated by library server 260 and downloaded to a client computer system 214, library server 260 uses its private library key 263 to apply a digital signature to the data block (see Column 14, lines 30-34).
2. After a data block is downloaded to a player 212/226 through a client computer system, the player 212/226 can retrieve the digital signature applied by the library server 260 by using a public server key known to the player 212/226. The player 212/226 can thereby verify that the downloaded data block originated with an authorized library server 260. The public server key is also known to the client computer system 214, which can perform the identical operation to verify that the downloaded data block originated with an authorized library server 260. The library server 260 performs signatures on the content (see Column 14, lines 39-48).

Accordingly, Katz et al. clearly discloses that a player 212/226 first downloads data blocks through a client computer system 214. Then, the player 212/226 retrieves the digital signature applied by the library server 260 by using a public server key known to the player 212/226. The player can then verify that the downloaded data block originated with an authorized library server 260. Similarly, as described above, the client computer system 214 performs the identical operation of verifying that the downloaded data block originated with an authorized library server 260 after the data has been downloaded to the client computer system 214, i.e., after a request for the downloaded data has been transmitted.

Therefore, Katz et al. clearly discloses that the player 212/226 or client computer system 214 first downloads data blocks. Next, in order to verify that the downloaded data blocks are from an authentic library server 260, the player 212/226 or client computer system 214 retrieves the digital signature applied by the library server 260. Thereafter, the player 212/226 or client computer system 214 can then verify that the downloaded data block is authentic, i.e., originated from an authorized library server 260.

Accordingly, Katz et al. clearly does not disclose or suggest that a retrieval request for retrieving the authenticated content data to the library server 260 only after

the content data has been authenticated by using the retrieved index data, as recited in each of claims 1, 6, 11 and 16. In fact, Katz et al. discloses the exact opposite authorization operation recited in claims 1, 6, 11 and 16. As described above, the player 212/226 or client computer system 214 determines the authenticity of the data only after the data has been downloaded, which is clearly in contrast to the retrieval and authentication operation recited in each of claims 1, 6, 11 and 16.

As mentioned above, the Examiner also cited Column 8, lines 32-40 of Katz to support his contention that content data retrieval is only requested if the authentication part has confirmed the authenticity of the content data. The Applicants respectfully submit that the Examiner's reliance on this portion of Katz et al. also does not justify the interpretation that Katz et al. discloses retrieving the content data only after the content data has been authenticated.

Column 8, lines 32-40 discloses that the library server 260 uses client information 272 stored therein to authenticate a request from the client computer system 214 to download data from the library server 260. However, the client information 272 of Katz et al. is only used to authenticate the client computer system 214, not the data itself. In other words, the library server 260 will not allow a requesting client computer system 214 to download data from the library server 260 if the client information 272 does not authenticate the requesting client computer system 214.

However, this operation of authenticating a client computer system 214 is markedly different from authenticating the data itself. Furthermore, as recited in each of claims 1, 6, 11 and 16, the authentication of the data is performed in the data terminal equipment, not the library server 260. Moreover, Column 8, lines 32-40 discloses that a request for the data precedes the authentication of the client computer system 214. In other words, the authentication of the requesting client computer system 214 is only performed after the requesting client computer system 214 has issued a request to download data from the library server 260.

As mentioned above, claims 1, 6, 11 and 16 each recite that a retrieval request for the data is only transmitted after the data has been authenticated. Accordingly, similar to Palage et al., Katz et al. clearly does not disclose or suggest transmitting a retrieval request for retrieving the content data to the server only if authenticity of the content data

has been confirmed, and receiving the authenticated content data from the server, as recited in claims 1, 6, 11 and 16.

Therefore, Katz et al. clearly does not cure the deficiencies of Palage et al. for failing to disclose or suggest each and every limitation of claims 1, 6, 11 and 16.

Accordingly, no obvious combination of Palage et al. and Katz et al. would result in the inventions of claims 1, 6, 11 and 16 since Palage et al. and Katz et al., either individually or in combination, clearly fail to disclose or suggest each and every limitation of claims 1, 6, 11 and 16.

Therefore, claims 1, 6, 11 and 16 are clearly allowable over Palage et al. and Katz et al.

In item 7 on page 4 of the Office Action, claims 5, 10, 15 and 20-24 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Palage et al. in view of Katz et al. and further in view of Moskowitz et al. (U.S. 5,905,800). Further, in item 9 on page 5 of the Office Action, claims 25-28 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Palage et al. in view of Katz et al. and further in view of Klug (U.S. 6,591,245).

As demonstrated above, Palage et al. and Katz et al. clearly fail to disclose or suggest each and every limitation of claims 1, 6, 11 and 16. Moskowitz et al. and Klug also fail to disclose or suggest transmitting a retrieval request for retrieving the content data to the server only if authenticity of the content data has been confirmed, and receiving the authenticated content data from the server, as recited in claims 1, 6, 11 and 16.

Therefore, neither Moskowitz et al. nor Klug cure the deficiencies of Palage et al. and Katz et al. for failing to disclose or suggest each and every limitation of claims 1, 6, 11 and 16.

Accordingly, no obvious combination of Palage et al., Klatz et al., Moskowitz et al. and Klug would result in the inventions of claims 1, 6, 11 and 16 since Palage et al., Klatz et al., Moskowitz et al. and Klug, either individually or in combination, clearly fail to disclose or suggest each and every limitation of claims 1, 6, 11 and 16.

Furthermore, it is submitted that the clear distinctions discussed above are such that a person having ordinary skill in the art at the time the invention was made would not

have been motivated to modify Palage et al., Klatz et al., Moskowitz et al. and Klug in such as manner as to result in, or otherwise render obvious, the present invention as recited in claims 1, 6, 11 and 16. Therefore, it is submitted that the claims 1, 6, 11 and 16, as well as claims 2-5, 7-10, 12-15 and 17-28 which depend therefrom, are clearly allowable over the prior art as applied by the Examiner.

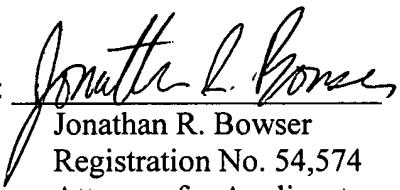
In view of the foregoing amendments and remarks, it is respectfully submitted that the present application is clearly in condition for allowance. An early notice thereof is respectfully solicited.

If, after reviewing this Amendment, the Examiner feels there are any issues remaining which must be resolved before the application can be passed to issue, the Examiner is respectfully requested to contact the undersigned by telephone in order to resolve such issues.

Respectfully submitted,

Masayuki KUMAZAWA et al.

By:


Jonathan R. Bowser
Registration No. 54,574
Attorney for Applicants

JRB/nrj
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
June 23, 2005